A graphical method to calculate Selmer groups of several families of non-CM elliptic curves

Fei Li and Derong Qiu *
(School of Mathematical Sciences,
Institute of Mathematics and Interdisciplinary Science,
Capital Normal University, Beijing 100048, P.R.China)

Abstract In this paper, we extend the ideas of Feng [F1], Feng-Xiong [FX] and Faulkner-James [FJ] to calculate the Selmer groups of elliptic curves $y^2 = x(x+\varepsilon pD)(x+\varepsilon qD)$.

Key words: elliptic curve, Selmer group, directed graph

2000 Mathematics Subject Classification: 11G05 (primary), 14H52, 14H25, 05C90(Secondary).

1 Introduction and Main Results

In this paper, we consider the following elliptic curves

$$E = E_{\varepsilon} : y^2 = x(x+\varepsilon pD)(x+\varepsilon qD), \qquad (1.1)$$
$$E' = E'_{\varepsilon} : y^2 = x^3 - 2\varepsilon(p+q)Dx^2 + 4^m D^2 x, \qquad (1.2)$$

where $\varepsilon = \pm 1$, p and q are odd prime numbers with $q - p = 2^m, m \geq 1$ and $D = D_1 \cdots D_n$ is a square-free integer with distinct primes $D_1, \cdots, D_n$. Moreover, $2 \nmid D$, $p \nmid D$ and $q \nmid D$. For each D_i, denote $\widehat{D_i} = D/D_i$ ($\widehat{D_1} = 1$ if $D = D_1$). We write $E = E_+, E' = E'_+$ if $\varepsilon = 1$, and $E = E_-, E' = E'_-$ if $\varepsilon = -1$.

* E-mail: derong@mail.cnu.edu.cn

There is an isogeny φ of degree 2 between E and E' as follows:

$$\varphi : E \longrightarrow E', \quad (x, y) \longmapsto (y^2/x^2,\ y(pqD^2 - x^2)/x^2).$$

The kernel is $E[\varphi] = \{O,\ (0, 0)\}$, and the dual isogeny of φ is

$$\widehat{\varphi} : E' \longrightarrow E, \quad (x, y) \longmapsto (y^2/4x^2,\ y(4^m D^2 - x^2)/8x^2)$$

with kernel $E'[\widehat{\varphi}] = \{O,\ (0, 0)\}$ (see [S, p.74]).

In this paper, we extend the ideas of Feng [F1], Feng-Xiong [FX] and Faulkner-James [FJ] to calculate the $\varphi(\widehat{\varphi})-$Selmer groups $S^{(\varphi)}(E/\mathbb{Q})$ and $S^{(\widehat{\varphi})}(E'/\mathbb{Q})$. The main results are as follows:

Theorem 1.1 Let $D = D_1D_2 \cdots D_sD_{s+1} \cdots D_n$ with $\left(\frac{pq}{D_i}\right) = 1\ (i \leq s)$ and $\left(\frac{pq}{D_j}\right) = -1\ (s < j \leq n)$ for some non-negative integer $s \leq n$. If m, p and D satisfy one of the following conditions:

(1) $m = 1,\ pD \equiv 5(\mathrm{mod}8)$ and $D \equiv 3(\mathrm{mod}4)$;

(2) $m = 1,\ pD \equiv 1(\mathrm{mod}8)$ and $D \equiv 1(\mathrm{mod}4)$; (3) $m = 2$;

(4) $pD \equiv 3(\mathrm{mod}8)$; (5) $m = 3,\ pD \equiv 1(\mathrm{mod}4)$; (6) $m = 4,\ pD \equiv 7(\mathrm{mod}8)$,

then $\sharp S^{(\varphi)}(E/\mathbb{Q}) = \sharp\{(V_1, V_2) \mapsto_e G(+D) :\ -1, p, q, D_k \notin V_1;\ s < k \leq n\}$. In the other cases, $\sharp S^{(\varphi)}(E/\mathbb{Q}) = \sharp\{(V_1, V_2) \mapsto_e G(+D) :\ -1, p, q, D_k \in V_2; s < k \leq n\} + \sharp\{(V_1, V_2) \mapsto_{qe} G(+D) :\ -1, p, q, D_k \notin V_1;\ s < k \leq n\}$. Here $G(+D)$ is the directed graph (see the following Definition 2.5).

Theorem 1.2. Let $D = D_1D_2 \cdots D_sD_{s+1} \cdots D_n$ with $\left(\frac{pq}{D_i}\right) = 1\ (i \leq s)$ and $\left(\frac{pq}{D_j}\right) = -1\ (s < j \leq n)$ for some non-negative integer $s \leq n$, then $\sharp S^{(\widehat{\varphi})}(E'/\mathbb{Q}) = 2\sharp\{(V_1, V_2) \mapsto_e g(+D) :\ \pm 2 \notin V_1\}$. Here $g(+D)$ is the directed graph (see the following Definition 2.8).

Theorem 1.3. Let $D = D_1D_2\cdots D_sD_{s+1}\cdots D_n$ with $\left(\frac{pq}{D_i}\right) = 1$ $(i \leq s)$ and $\left(\frac{pq}{D_j}\right) = -1$ $(s < j \leq n)$ for some non-negative integer $s \leq n$. If m, p and D satisfy one of the following conditions:

(1) $m = 1,\ pD \equiv 5, 7(\text{mod}8)$ and $D \equiv 3(\text{mod}4)$;

(2) $m = 1,\ pD \equiv \pm 3(\text{mod}8)$ and $D \equiv 1(\text{mod}4)$;

(3) $m = 2$; (4) $m = 3,\ pD \not\equiv 1(\text{mod}8)$;

(5) $m = 4,\ pD \equiv 1(\text{mod}4)$, (6) $m \geq 5,\ pD \equiv 5(\text{mod}8)$,

then $\sharp S^{(\varphi)}(E/\mathbb{Q}) = \sharp\{(V_1, V_2) \mapsto_e G(-D) :\ p, q, D_k \in V_2; s < k \leq n\}$; In other cases, $\sharp S^{(\varphi)}(E/\mathbb{Q}) = \sharp\{(V_1, V_2) \mapsto_e G(-D) :\ p, q, D_k \in V_2; s < k \leq n\} + \sharp\{(V_1, V_2) \mapsto_{qe} G(-D) :\ p, q, D_k \in V_2; s < k \leq n\}$. Here $G(-D)$ is the directed graph (see the following Definition 2.10).

Theorem 1.4. Let $D = D_1D_2\cdots D_sD_{s+1}\cdots D_n$ with $\left(\frac{pq}{D_i}\right) = 1$ $(i \leq s)$ and $\left(\frac{pq}{D_j}\right) = -1$ $(s < j \leq n)$ for some non-negative integer $s \leq n$, then $\sharp S^{(\widehat{\varphi})}(E'/\mathbb{Q}) = 2\sharp\{(V_1, V_2) \mapsto_e g(-D) :\ -1, \pm 2 \notin V_1\}$. Here $g(-D)$ is the directed graph (see the following Definition 2.13).

Moreover, another result about the Selmer group of elliptic curves in (1.1) for all integers $m \geq 2$ is given in the appendix.

2 Proofs of Theorems

Let $M_{\mathbb{Q}}$ be the set of all places of $\mathbb{Q}$, including the infinite ∞. For each place p, denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ at p, and if p is finite, denote by v_p the corresponding normalized additive valuation, so $v_p(p) = 1$. Let $S = \{\infty, 2, p, q, D_1, \cdots, D_n\}$, and define a subgroup of $\mathbb{Q}^\star/\mathbb{Q}^{\star^2}$ as follows: $\mathbb{Q}(S, 2) =< -1 > \times < 2 > \times < p >$

$\times < q > \times < D_1 > \times \cdots \times < D_n > \cong (\mathbb{Z}/2\mathbb{Z})^{n+4}$. For any subset $A \subset \mathbb{Q}^\star$, we write $< A >$ for the subgroup of $\mathbb{Q}^\star/\mathbb{Q}^{\star^2}$ generated by all the elements in A. For each $d \in \mathbb{Q}(S,2)$, define the curves

$C_d:\ dw^2 = d^2 - 2\varepsilon(p+q)Ddz^2 + 4^m D^2 z^4$, and

$C'_d:\ dw^2 = d^2 + \varepsilon(p+q)Ddz^2 + pqD^2 z^4$.

We have the following propositions 2.1 $\sim$ 2.4 in determining the local solutions of these curves C_d and C'_d. The proofs are similar to those in [LQ], so we omit the details.

Proposition 2.1 We assume $\varepsilon = 1$ and the elliptic curve $E = E_+$ be as in (1.1).

(A) For $d \in \mathbb{Q}(S,2)$, if one of the following conditions holds:

(1) $d < 0$; (2) $p \mid d$; (3) $q \mid d$.

Then $d \notin S^{(\varphi)}(E/\mathbb{Q})$. Moreover, if $d > 0$, then $C_d(\mathbb{R}) \neq \emptyset$.

(B) For each $d > 0, 2 \mid d \mid 2D, d \in \mathbb{Q}(S,2)$, we have

(1) if $m = 1$, then $C_d(\mathbb{Q}_2) \neq \emptyset \iff \frac{d}{2} - 2D(p+1) + \frac{2D^2}{d} \equiv 2(\mathrm{mod}16)$;

if $m = 2$, then $C_d(\mathbb{Q}_2) = \emptyset$;

if $m = 3$, then $C_d(\mathbb{Q}_2) \neq \emptyset \iff d - D(p+4) + \frac{4D^2}{d} \equiv 1(\mathrm{mod}8)$;

if $m = 4$, then $C_d(\mathbb{Q}_2) \neq \emptyset \iff d - Dp \equiv 1(\mathrm{mod}8)$;

if $m \geq 5$, then $C_d(\mathbb{Q}_2) \neq \emptyset \iff Dp \equiv 7(\mathrm{mod}8)$ or $d - Dp \equiv 1(\mathrm{mod}8)$.

(2) For each odd prime number $l \mid \frac{2pqD}{d}$, $C_d(\mathbb{Q}_l) \neq \emptyset \iff \left(\frac{d}{l}\right) = 1$.

(3) For each odd prime number $l \mid d$, $C_d(\mathbb{Q}_l) \neq \emptyset \iff \left(\frac{pDdl^{-2}}{l}\right) = \left(\frac{qDdl^{-2}}{l}\right) = 1$.

(C) For $d>0, d \mid D, d \in \mathbb{Q}(S,2)$, we have

(1) if $m=1$, then $C_d(\mathbb{Q}_2) \neq \emptyset \iff d \equiv 1 (\mathrm{mod} 4)$;

if $m=2$, then $C_d(\mathbb{Q}_2) \neq \emptyset \iff d \equiv 1 (\mathrm{mod} 4)$ or $2d - D(p+2) \equiv 1 (\mathrm{mod} 8)$;

if $m \geq 3$, then $C_d(\mathbb{Q}_2) \neq \emptyset \iff d \equiv 1 (\mathrm{mod} 4)$ or $d - Dp \equiv 0 (\mathrm{mod} 4)$.

(2) For each prime number $l \mid \frac{pqD}{d}$, $C_d(\mathbb{Q}_l) \neq \emptyset \iff \left(\frac{d}{l}\right) = 1$.

(3) For each prime number $l \mid d$, $C_d(\mathbb{Q}_l) \neq \emptyset \iff \left(\frac{pdDl^{-2}}{l}\right) = \left(\frac{qdDl^{-2}}{l}\right) = 1$.

Proposition 2.2 We assume $\varepsilon = 1$ and the elliptic curve $E' = E'_+$ be as in (1.2).

(A) (1) For any $d \in \mathbb{Q}(S,2)$, $C'_d(\mathbb{R}) \neq \emptyset$. If $2 \mid d$, then $d \notin S^{(\widehat{\varphi})}(E'/\mathbb{Q})$.

(2) $\{1, pq, -pD, -qD\} \subset S^{(\widehat{\varphi})}(E'/\mathbb{Q})$.

(B) For each $d \in \mathbb{Q}(S,2)$ satisfying $d \mid pD$, we have

(B1) (1) If $m=1$, then $C'_d(\mathbb{Q}_2) \neq \emptyset$ if and only if one of the following conditions holds: (a) $d \equiv 1 (\mathrm{mod} 8)$, (b) $(d+pD)(d+qD) \equiv 0 (\mathrm{mod} 16)$, (c) $\frac{pqD^2}{d} \equiv 1 (\mathrm{mod} 8)$;

(2) If $m=2$, then $C'_d(\mathbb{Q}_2) \neq \emptyset$ if and only if one of the following conditions holds:

(a) $d \equiv 1 (\mathrm{mod} 8)$, (b) $\frac{pqD^2}{d} \equiv 1 (\mathrm{mod} 8)$,

(c) $d + pD \equiv 0 (\mathrm{mod} 4)$, (d) $d \equiv 3 (\mathrm{mod} 4)$ and $(p+2)D \equiv 1 (\mathrm{mod} 8)$;

(3) If $m=3$, then $C'_d(\mathbb{Q}_2) \neq \emptyset$ if and only if one of the following conditions holds:

(a) $d \equiv 1 (\mathrm{mod} 8)$, (b) $\frac{pqD^2}{d} \equiv 1 (\mathrm{mod} 8)$, (c) $d + pD \equiv 0 (\mathrm{mod} 8)$,

(d) $d \equiv 3 (\mathrm{mod} 4)$, and $d+pD \equiv 4 (\mathrm{mod} 8)$, (e) $d \equiv 5 (\mathrm{mod} 8)$ and $d+pD \equiv 2 (\mathrm{mod} 4)$;

(4) If $m=4$, then $C'_d(\mathbb{Q}_2) \neq \emptyset$ if and only if one of the following conditions holds:

(a) $d \equiv 1 (\mathrm{mod} 8)$, (b) $\frac{pqD^2}{d} \equiv 1 (\mathrm{mod} 8)$, (c) $d + pD \equiv 0 (\mathrm{mod} 8)$,

(d) $d \equiv 1(\bmod 8)$ and $d{+}pD \equiv 2(\bmod 4)$, (e) $d \equiv 5(\bmod 8)$ and $d{+}pD \equiv 4(\bmod 8)$;

(5) If $m \geq 5$, then $C'_d(\mathbb{Q}_2) \neq \emptyset$ if and only if one of the following conditions holds:

(a) $d \equiv 1(\bmod 8)$, (b) $\frac{pqD^2}{d} \equiv 1(\bmod 8)$, (c) $d + pD \equiv 0(\bmod 8)$.

(B2) $C'_d(\mathbb{Q}_p) \neq \emptyset$ and $C'_d(\mathbb{Q}_q) \neq \emptyset$.

(B3) For each prime $l \mid D, l \nmid d$, $\quad C'_d(\mathbb{Q}_l) \neq \emptyset \Longleftrightarrow \left(1 - \left(\frac{d}{l}\right)\right)\left(1 - \left(\frac{pqd}{l}\right)\right) = 0$.

(B4) For each prime $l \mid D, l \mid d$, $C'_d(\mathbb{Q}_l) \neq \emptyset \Longleftrightarrow \left(1 - \left(\frac{-pdDl^{-2}}{l}\right)\right)\left(1 - \left(\frac{-qdDl^{-2}}{l}\right)\right) = 0$.

Proposition 2.3 We assume $\varepsilon = -1$ and the elliptic curve $E = E_-$ be as in (1.1).

(A) For $d \in \mathbb{Q}(S, 2)$, if one of the following conditions holds:

(1) $p \mid d$; (2) $q \mid d$.

Then $d \notin S^{(\varphi)}(E/\mathbb{Q})$. Moreover, $C_d(\mathbb{R}) \neq \emptyset$.

(B) For each $2 \mid d, d \mid 2D, d \in \mathbb{Q}(S, 2)$, we have

(1) if $m = 1$, then $C_d(\mathbb{Q}_2) \neq \emptyset \Longleftrightarrow \frac{d}{2} + 2D(p+1) + \frac{2D^2}{d} \equiv 2(\bmod 16)$;

if $m = 2$, then $C_d(\mathbb{Q}_2) = \emptyset$;

if $m = 3$, then $C_d(\mathbb{Q}_2) \neq \emptyset \Longleftrightarrow d + D(p+4) + \frac{4D^2}{d} \equiv 1(\bmod 8)$;

if $m = 4$, then $C_d(\mathbb{Q}_2) \neq \emptyset \Longleftrightarrow d + Dp \equiv 1(\bmod 8)$;

if $m \geq 5$, then $C_d(\mathbb{Q}_2) \neq \emptyset \Longleftrightarrow Dp \equiv 1(\bmod 8)$ or $d + Dp \equiv 1(\bmod 8)$.

(2) For each odd prime number $l \mid \frac{2pqD}{d}$, $C_d(\mathbb{Q}_l) \neq \emptyset \Longleftrightarrow \left(\frac{d}{l}\right) = 1$.

(3) For each odd prime number $l \mid d$, $C_d(\mathbb{Q}_l) \neq \emptyset \Longleftrightarrow \left(\frac{-pdDl^{-2}}{l}\right) = \left(\frac{-qdDl^{-2}}{l}\right) = 1$.

(C) For $d \mid D, d \in \mathbb{Q}(S, 2)$, we have

(1) if $m = 1$, then $C_d(\mathbb{Q}_2) \neq \emptyset \Longleftrightarrow d \equiv 1(\bmod 4)$;

if $m=2$, then $C_d(\mathbb{Q}_2)\neq\emptyset \iff d\equiv 1(\mathrm{mod}4)$ or $2d+D(p+2)\equiv 1(\mathrm{mod}8)$;

if $m\geq 3$, then $C_d(\mathbb{Q}_2)\neq\emptyset \iff d\equiv 1(\mathrm{mod}4)$ or $d+Dp\equiv 0(\mathrm{mod}4)$.

(2) For each prime number $l\mid \frac{pqD}{d}$, $C_d(\mathbb{Q}_l)\neq\emptyset \iff \left(\frac{d}{l}\right)=1$.

(3) For each prime number $l\mid d$, $C_d(\mathbb{Q}_l)\neq\emptyset \iff \left(\frac{-pdDl^{-2}}{l}\right)=\left(\frac{-qdDl^{-2}}{l}\right)=1$.

Proposition 2.4. We assume $\varepsilon=-1$ and the elliptic curve $E'=E'_-$ be as in (1.2).

(A) (1) For any $d\in\mathbb{Q}(S,2)$ and $d>0$, $C'_d(\mathbb{R})\neq\emptyset$. If $2\mid d$ or $d<0$, then $d\notin S^{(\widehat{\varphi})}(E'/\mathbb{Q})$.

(2) $\{1,pq,pD,qD\}\subset S^{(\widehat{\varphi})}(E'/\mathbb{Q})$.

(B) For each $d\in\mathbb{Q}(S,2), d\mid pD, d>0$, we have

(B1) (1) If $m=1$, then $C'_d(\mathbb{Q}_2)\neq\emptyset$ if and only if one of the following conditions holds:

(a) $d\equiv 1(\mathrm{mod}8)$, (b) $(d-pD)(d-qD)\equiv 0(\mathrm{mod}16)$, (c) $\frac{pqD^2}{d}\equiv 1(\mathrm{mod}8)$;

(2) If $m=2$, then $C'_d(\mathbb{Q}_2)\neq\emptyset$ if and only if one of the following conditions holds:

(a) $d\equiv 1(\mathrm{mod}8)$, (b) $\frac{pqD^2}{d}\equiv 1(\mathrm{mod}8)$,

(c) $d-pD\equiv 0(\mathrm{mod}4)$, (d) $d\equiv 3(\mathrm{mod}4)$ and $(p+2)D\equiv 7(\mathrm{mod}8)$;

(3) If $m=3$, then $C'_d(\mathbb{Q}_2)\neq\emptyset$ if and only if one of the following conditions holds:

(a) $d\equiv 1(\mathrm{mod}8)$, (b) $\frac{pqD^2}{d}\equiv 1(\mathrm{mod}8)$, (c) $d-pD\equiv 0(\mathrm{mod}8)$,

(d) $d\equiv 3(\mathrm{mod}4)$ and $d-pD\equiv 4(\mathrm{mod}8)$, (e) $d\equiv 5(\mathrm{mod}8)$ and $d-pD\equiv 2(\mathrm{mod}4)$.

(4) If $m=4$, then $C'_d(\mathbb{Q}_2)\neq\emptyset$ if and only if one of the following conditions holds:

(a) $d\equiv 1(\mathrm{mod}8)$, (b) $\frac{pqD^2}{d}\equiv 1(\mathrm{mod}8)$, (c) $d-pD\equiv 0(\mathrm{mod}8)$,

(d) $d\equiv 1(\mathrm{mod}8)$ and $d-pD\equiv 2(\mathrm{mod}4)$, (e) $d\equiv 5(\mathrm{mod}8)$ and $d-pD\equiv 4(\mathrm{mod}8)$;

(5) If $m \geq 5$, then $C'_d(\mathbb{Q}_2) \neq \emptyset$ if and only if one of the following conditions holds:

(a) $d \equiv 1 (\bmod 8)$, (b) $\frac{pqD^2}{d} \equiv 1 (\bmod 8)$, (c) $d - pD \equiv 0 (\bmod 8)$.

(B2) $C'_d(\mathbb{Q}_p) \neq \emptyset$ and $C'_d(\mathbb{Q}_q) \neq \emptyset$.

(B3) For each prime $l \mid D, l \nmid d$, $\quad C'_d(\mathbb{Q}_l) \neq \emptyset \Longleftrightarrow \left(1 - \left(\frac{d}{l}\right)\right)\left(1 - \left(\frac{pqd}{l}\right)\right) = 0$.

(B4) For each prime $l \mid D, l \mid d$, $C'_d(\mathbb{Q}_l) \neq \emptyset \Longleftrightarrow \left(1 - \left(\frac{pdDl^{-2}}{l}\right)\right)\left(1 - \left(\frac{qdDl^{-2}}{l}\right)\right) = 0$.

Now let $G = (V, E)$ be a directed graph. Recall that a partition (V_1, V_2) of V is called even if for any vertex, $P \in V_2(V_1), \sharp\{P \to V_1(V_2)\}$ is even. In this case, we shall write $(V_1, V_2) \mapsto_e V$. The partition (V_1, V_2) is called quasi-even if for any vertex, $P \in V_1(V_2)$,

$$\sharp\{P \to V_2(V_1)\} \equiv \begin{cases} 0 (\bmod 2) & \text{if } \left(\frac{2}{P}\right) = 1, \\ 1 (\bmod 2) & \text{if } \left(\frac{2}{P}\right) = -1. \end{cases}$$

In this case, we shall write $(V_1, V_2) \mapsto_{qe} V$ (see [F2] and [FJ] for these definitions and related facts). Throughout this paper, for convenience, we write empty product as 1.

Definition 2.5 Let $D = D_1 D_2 \cdots D_s D_{s+1} \cdots D_n$ with $\left(\frac{pq}{D_i}\right) = 1$ $(i \leq s)$ and $\left(\frac{pq}{D_j}\right) = -1$ $(s < j \leq n)$ for some non-negative integer $s \leq n$. A directed graph G(+D) is defined as follows:

Case 1. If m, p and D satisfy one of the following conditions:

(1) $m = 1$; (2) $m = 2, (p+2)D \not\equiv 5 (\bmod 8)$; (3) $m \geq 3, pD \equiv 1 (\bmod 4)$, then define the directed graph $G(+D) = G_1(+D)$ by defining the vertex $V(G(+D))$ to be $V(G_1(+D)) = \{-1, p, q, D_1, D_2, \cdots, D_n\}$ and the edges

$E(G(+D))$ as $E(G_1(+D)) = \{\overrightarrow{D_i D_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s, 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_j D_i} :$

$\left(\frac{D_i}{D_j}\right) = -1, 1 \leq i \leq s, s < j \leq n\} \bigcup \{\overrightarrow{lD_i} : \left(\frac{D_i}{l}\right) = -1, 1 \leq i \leq s, l = p, q\} \bigcup \{\overrightarrow{-1D_i} : \left(\frac{-1}{D_i}\right) = -1,\ 1 \leq i \leq s\} \bigcup \{\overrightarrow{D_i p} : \left(\frac{p}{D_i}\right) = -1,\ 1 \leq i \leq s\}$.

Case 2. If m, p and D satisfy one of the following conditions:

(1) $m = 2, (p+2)D \equiv 5(\mathrm{mod} 8)$; (2) $m \geq 3, pD \equiv 3(\mathrm{mod} 4)$, then define the directed graph $G(+D) = G_2(+D)$ by defining the vertex $V(G(+D))$ to be $V(G_2(+D)) = \{p, q, D_1, D_2, \cdots, D_n\}$ and the edges $E(G(+D))$ as

$E(G_5^2(+D)) = \{\overrightarrow{D_i D_j} : \left(\frac{D_j}{D_i}\right) = -1,\ 1 \leq i \leq s, 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_j D_i} : \left(\frac{D_i}{D_j}\right) = -1,\ 1 \leq i \leq s,\ s < j \leq n\} \bigcup \{\overrightarrow{lD_i} : \left(\frac{D_i}{l}\right) = -1,\ 1 \leq i \leq s,\ l = p, q\} \bigcup \{\overrightarrow{D_i p} : \left(\frac{p}{D_i}\right) = -1,\ 1 \leq i \leq s\}$.

Here we define $\left(\frac{2}{-1}\right) = 1$, if m, p and D satisfy one of the following conditions:

(1) $m = 1,\ pD \equiv 7(\mathrm{mod} 8)$ and $D \equiv 1(\mathrm{mod} 4)$;

(2) $m = 1,\ pD \equiv 1(\mathrm{mod} 8)$ and $D \equiv 3(\mathrm{mod} 4)$; (3) $m \geq 4, pD \equiv 1(\mathrm{mod} 8)$.

And we define $\left(\frac{2}{-1}\right) = -1$, if m, p and D satisfy one of the following conditions:

(1) $m = 1,\ pD \equiv 5(\mathrm{mod} 8)$ and $D \equiv 1(\mathrm{mod} 4)$;

(2) $m = 1,\ pD \equiv 7(\mathrm{mod} 8)$ and $D \equiv 3(\mathrm{mod} 4)$; (3) $m \geq 4, pD \equiv 5(\mathrm{mod} 8)$.

Lemma 2.6. For every even partition (V_1, V_2) of $G(+D)$ such that V_1 contains no $-1, p, q$ or D_k $(s < k \leq n)$, we have $d \in S^{(\varphi)}(E/\mathbb{Q})$ where $d = \prod_{P_0 \in V_1} P_0$. Conversely, suppose d is odd and $d \in S^{(\varphi)}(E/\mathbb{Q})$, we may write $d = P_1 P_2 \cdots P_t$ with $1 \leq t \leq s$ for distinct $P_j \in V(G(+D))$ $(1 \leq j \leq t)$, then (V_1, V_2) is even, where $V_1 = \{P_1, P_2, \cdots, P_t\}$.

Proof. Suppose (V_1, V_2) is a nontrivial even partition of $G(+D)$ such that $-1, p, q, D_k \notin V_1$ $(s < k \leq n)$. Let $V_1 = \{D_1, D_1, \cdots, D_t\}$ for some $1 \leq t \leq s$. Consider $d = D_1 D_2 \cdots D_t$. For any $1 \leq i \leq t$, we have $\left(\frac{pdDD_i^{-2}}{D_i}\right) = (-1)^{\sharp\{\overrightarrow{D_i P} : P \in V_2\}} =$

1 since (V_1, V_2) is even. Therefore, $C_d(\mathbb{Q}_{D_i}) \neq \emptyset$ by Proposition 2.1(C)(3). Also, for $P \in V_2, P \neq -1, \left(\frac{d}{P}\right) = (-1)^{\sharp\{\overrightarrow{PD_i}:\ D_i \in V_1\}} = 1$ since (V_1, V_2) is even. Therefore, $C_d(\mathbb{Q}_P) \neq \emptyset$ by Proposition 2.1(C)(2). We claim that $C_d(\mathbb{Q}_2) \neq \emptyset$ since (V_1, V_2) is even. For an example in case 1, $m = 1$: because $\sharp\{\overrightarrow{-1D_i}:\ D_i \in V_1\}$ is even, $d \equiv 1 \bmod 4$. Therefore, $C_d(\mathbb{Q}_2) \neq \emptyset$ by Proposition 2.1(C)(1). The remaining cases can be done similarly. And by Proposition 2.1(A), we have d in $S^{(\varphi)}(E/\mathbb{Q})$.

Conversely, suppose $d = P_1P_2 \cdots P_t \in S^{(\varphi)}(E/\mathbb{Q})$ and d is odd. By Proposition 2.1(C), $P_i \in \{D_1, D_2, \cdots, D_s\}$ and $\left(\frac{pdDP_i^{-2}}{P_i}\right) = 1$ for each $1 \leq i \leq t$. Let $V_1 = \{P_1, P_2, \cdots, P_t\}$. Therefore, $1 = \left(\frac{pdDP_i^{-2}}{P_i}\right) = (-1)^{\sharp\{\overrightarrow{P_iP}:\ P \in V_2\}}$ for $1 \leq i \leq t$. So we get $\sharp\{\overrightarrow{P_iP} : P \in V_2\}$ is even. For prime $P \mid pqDd^{-1}$, we have $P \in V_2$ and $\left(\frac{d}{P}\right) = 1$. Therefore, $1 = \left(\frac{d}{P}\right) = (-1)^{\sharp\{\overrightarrow{PP_i}:\ P_i \in V_1\}}$, which shows that $\sharp\{\overrightarrow{PP_i}:\ P_i \in V_1\}$ is even. If $-1 \in V_2$ in case 1, then $d \equiv 1 \bmod 4$ for $C_d(\mathbb{Q}_2) \neq \emptyset$. Hence $\sharp\{\overrightarrow{-1P_i}:\ 1 \leq i \leq t\}$ is even. To sum up, (V_1, V_2) is even. The proof of lemma 2.6 is completed. $\square$

Lemma 2.7. For every quasi-even partition (V_1, V_2) of $G(+D)$ such that V_1 contains no $-1, p, q$ or D_k $(s < k \leq n)$, we have $2d \in S^{(\varphi)}(E/\mathbb{Q})$, where $d = \prod_{P_0 \in V_1} P_0$. Conversely, If d is even and $d \in S^{(\varphi)}(E/\mathbb{Q})$, we may write $d = 2P_1P_2 \cdots P_t$ with $1 \leq t \leq s$ for distinct $P_j \in V(G(+D))$ $(1 \leq j \leq t)$, then (V_1, V_2) is quasi-even, where $V_1 = \{P_1, P_2, \cdots, P_t\}$.

Proof. Suppose (V_1, V_2) is a nontrivial quasi-even partition of $G(+D)$ such that $-1, p, q, D_k \notin V_1$ $(s < k \leq n)$. Let $V_1 = \{D_1, D_1, \cdots, D_t\}$ for some $1 \leq t \leq s$. Consider $2d = 2D_1D_2 \cdots D_t$. For any $1 \leq i \leq t$, we have $\left(\frac{2pdDD_i^{-2}}{D_i}\right) = \left(\frac{2}{D_i}\right)(-1)^{\sharp\{\overrightarrow{D_iP}:\ P \in V_2\}} = 1$ since (V_1, V_2) is quasi-even. Therefore, $C_{2d}(\mathbb{Q}_{D_i}) \neq \emptyset$ by Proposition 2.1(B)(3). Also, for $P \in V_2$ and $P \neq -1$, $\left(\frac{2d}{P}\right) = \left(\frac{2}{P}\right)(-1)^{\sharp\{\overrightarrow{PD_i}:D_i \in V_1\}} =$

1 since (V_1, V_2) is quasi-even. Therefore, $C_{2d}(\mathbb{Q}_P) \neq \emptyset$ by Proposition 2.1(B)(2). We assert that $C_{2d}(\mathbb{Q}_2) \neq \emptyset$. To see this, we only need to prove case 1 with $m = 1, D \equiv 1 (\mathrm{mod} 4)$ and $pD \equiv 7(\mathrm{mod} 8)$, the other cases can be similarly done. Firstly, since $\left(\frac{2}{-1}\right) = 1$, we have $\sharp\{\overrightarrow{-1D_i} : \ 1 \leq i \leq t\}$ is even. So $d \equiv 1 \mathrm{mod} 4$ and $2D(2d)^{-1} \equiv 1 \mathrm{mod} 4$. Next, since $pD \equiv 7(\mathrm{mod} 8)$, we have $d(1 - 2D(2d)^{-1})^2 - 2pD \equiv 2(\mathrm{mod} 16)$, i.e., $d - 2D(p+1) + \frac{2D^2}{2d} \equiv 2(\mathrm{mod} 16)$, which shows that $C_{2d}(\mathbb{Q}_2) \neq \emptyset$ by Proposition 2.1(B)(1). Furthermore by Proposition 2.1(A), we get $2d \in S^{(\varphi)}(E/\mathbb{Q})$.

Conversely, suppose $d = 2P_1P_2 \cdots P_t \in S^{(\varphi)}(E/\mathbb{Q})$. By Proposition 2.1(B), $P_i \in \{D_1, D_2, \cdots, D_s\}$ and $\left(\frac{pdDP_i^{-2}}{P_i}\right) = 1$ for each $1 \leq i \leq t$. Let $V_1 = \{P_1, P_2, \cdots, P_t\}$. Therefore, $1 = \left(\frac{pdDP_i^{-2}}{P_i}\right) = \left(\frac{2}{P_i}\right)(-1)^{\sharp\{\overrightarrow{P_iP}: \ P \in V_2\}}$ for $1 \leq i \leq t$. So $\sharp\{P_i \to V_2\} = 0(\mathrm{mod} 2)$, if $\left(\frac{2}{P_i}\right) = 1$ or $1(\mathrm{mod} 2)$, if $\left(\frac{2}{P_i}\right) = -1$. For prime $P \mid 2pqDd^{-1}$, we have $P \in V_2$ and $\left(\frac{d}{P}\right) = 1$. Therefore, $1 = \left(\frac{d}{P}\right) = \left(\frac{2}{P_i}\right)(-1)^{\sharp\{\overrightarrow{PP_i}: \ P_i \in V_1\}}$, which shows that $\sharp\{P \to V_1\} = 0(\mathrm{mod} 2)$, if $\left(\frac{2}{P}\right) = 1$ or $1(\mathrm{mod} 2)$, if $\left(\frac{2}{P}\right) = -1$. If $-1 \in V_2$ in case 1, e.g., $m = 1, \ D \equiv 1(\mathrm{mod} 4)$ and $pD \equiv 7(\mathrm{mod} 8)$: for $C_{2d}(\mathbb{Q}_2) \neq \emptyset$, by Proposition 2.1(A) we have $d \equiv 1(\mathrm{mod} 4)$. Hence $\sharp\{\overrightarrow{-1P_i} : \ 1 \leq i \leq t\}$ is even (Here notice that $\left(\frac{2}{-1}\right) = 1$). The remaining cases can be done similarly. To sum up, (V_1, V_2) is quasi-even. The proof of lemma 2.7 is completed. $\square$

Proof of Theorem 1.1. By Proposition 2.1, $S^{(\varphi)}(E/\mathbb{Q}) \subset \{2, D_1, D_2, \cdots, D_n\}$. Furthermore, by lemma 2.6 and lemma 2.7, it is easy to obtain all the corresponding results for different m, p, D. The proof is completed. $\square$

Definition 2.8. Let $D = D_1D_2 \cdots D_sD_{s+1} \cdots D_n$ with $\left(\frac{pq}{D_i}\right) = 1 \ (i \leq s)$ and $\left(\frac{pq}{D_j}\right) = -1 \ (s < j \leq n)$ for some non-negative integer $s \leq n$. A graph directed g(+D) is defined as follows :

Case 1. If m, p and D satisfy one of the following conditions:

(1) $m = 1, p \equiv 1(\text{mod}4)$ and $p - D \equiv 0, 6(\text{mod}8)$;

(2) $m = 1, p \equiv 3(\text{mod}4)$ and $p - D \equiv 2, 4(\text{mod}8)$;

(3) $m = 2, pD \equiv 1(\text{mod}4)$; (4) $m = 2, D \equiv 3(\text{mod}4)$ and $pD \equiv 3(\text{mod}8)$;

(5) $m = 2, D \equiv 1(\text{mod}4)$ and $pD \equiv 7(\text{mod}8)$; (6) $m = 3, pD \equiv 1(\text{mod}4)$,

then define the directed graph $g(+D) = g_1(+D)$ by defining the vertex $V(g(+D))$ to be $V(g_1(+D)) = \{-1, p, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(+D))$ as $E(g_1(+D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s, 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_i - 1} : \left(\frac{-1}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \leq i \leq s\}$.

Case 2. If m, p and D satisfy one of the following conditions:

(1) $m = 1, p \equiv 1(\text{mod}4)$ and $p - D \equiv 2, 4(\text{mod}8)$; (2) $m \geq 4, pD \equiv 5(\text{mod}8)$,

then define the directed graph $g(+D) = g_2(+D)$ by defining the vertex $V(g(+D))$ to be $V(g_2(+D)) = \{-1, -2, p, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(+D))$ as $E(g_2(+D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s, 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_i - 1} : \left(\frac{-1}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{-2D_k} : \left(\frac{-2}{D_k}\right) = -1, 1 \leq k \leq n\} \bigcup \{\overrightarrow{-2p} : \left(\frac{-2}{p}\right) = -1 \bigcup \{\overrightarrow{-2 - 1}\}$.

Case 3. If m, p and D satisfy one of the following conditions:

(1) $m = 1, p \equiv 3(\text{mod}4)$ and $p - D \equiv 0, 6(\text{mod}8)$; (2) $m \geq 4, pD \equiv 1(\text{mod}8)$,

then define the directed graph $g(+D) = g_3(+D)$ by defining the vertex $V(g(+D))$ to be $V(g_3(+D)) = \{-1, p, 2, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(+D))$ as $E(g_3(+D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s, 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_i - 1} : \left(\frac{-1}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{2D_k} : \left(\frac{2}{D_k}\right) = -1, 1 \leq k \leq n\} \bigcup \{\overrightarrow{2p} : \left(\frac{2}{p}\right) = -1\}$.

Case 4. If m, p and D satisfy one of the following conditions:

(1) $m = 2, D \equiv 1(\mathrm{mod}4)$ and $pD \equiv 3(\mathrm{mod}8)$;

(2) $m = 2, D \equiv 3(\mathrm{mod}4)$ and $pD \equiv 7(\mathrm{mod}8)$;

(3) $m = 3, pD \equiv 3(\mathrm{mod}8)$; (4) $m = 4, pD \equiv 3(\mathrm{mod}4)$; (5) $m \geq 5, pD \equiv 3(\mathrm{mod}8)$,

then define the directed graph $g(+D) = g_4(+D)$ by defining the vertex $V(g(+D))$ to be $V(g_4(+D)) = \{-1, p, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(+D))$ as $E(g_4(+D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s, 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_i - 1} : \left(\frac{-1}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{-1D_k} : \left(\frac{-1}{D_k}\right) = -1, 1 \leq k \leq n\} \bigcup \{\overrightarrow{-1p} : \left(\frac{-1}{p}\right) = -1\}$.

Case 5. If m, p and D satisfy one of the following conditions:

(1) $m = 3, pD \equiv 7(\mathrm{mod}8)$; (2) $m \geq 5, pD \equiv 7(\mathrm{mod}8)$,

then define the directed graph $g(+D) = g_5(+D)$ by defining the vertex $V(g(+D))$ to be $V(g_5(+D)) = \{-1, p, -2, 2, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(+D))$ as $E(g_5(+D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s, 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_i - 1} : \left(\frac{-1}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{-2D_k} : \left(\frac{-2}{D_k}\right) = -1, 1 \leq k \leq n\} \bigcup \{\overrightarrow{-2p} : \left(\frac{-2}{p}\right) = -1\} \bigcup \{\overrightarrow{2D_k} : \left(\frac{2}{D_k}\right) = -1, 1 \leq k \leq n\} \bigcup \{\overrightarrow{2p} : \left(\frac{2}{p}\right) = -1\} \bigcup \{\overrightarrow{-2 - 1}\}$.

Lemma 2.9. For every even partition (V_1, V_2) of $g(+D)$ such that V_1 contains no ± 2, we have $d \in S^{(\widehat{\varphi})}(E'/\mathbb{Q})$, where $d = \prod_{P_0 \in V_1} P_0$. Conversely, if d is odd and $d \in S^{(\widehat{\varphi})}(E'/\mathbb{Q})$, we may write $d = P_1P_2 \cdots P_t$ for distinct $P_j \in V(g(+D))$ $(1 \leq j \leq t)$, then (V_1, V_2) is even, where $V_1 = \{P_1, P_2, \cdots, P_t\}$.

Proof. Suppose (V_1, V_2) is a nontrivial even partition of $g(+D)$ such that $\pm 2 \notin V_1$. Let $V_1 = \{P_1, P_1, \cdots, P_t\}, P_i \in \{-1, p, D_1, D_2, \cdots, D_n\}$ for each $1 \leq i \leq s$.

Consider $d = P_1P_2\cdots P_t$. For each prime $l \mid \gcd(D,\ d)$, if $l \in \{D_j:\ \ s < j \leq n\}$, $(\left(\frac{-pdDl^{-2}}{l}\right)-1)(\left(\frac{-qdDl^{-2}}{l}\right)-1)=0$ because $\left(\frac{-pdDl^{-2}}{l}\right)\left(\frac{-qdDl^{-2}}{l}\right)=\left(\frac{pq}{l}\right)=-1$; if $l \in \{D_i:\ \ 1\leq i\leq s\}$, then $\left(\frac{-pdDl^{-2}}{l}\right) = (-1)^{\sharp\{\overrightarrow{lP}:\ P\in V_2\}} = 1$ because (V_1, V_2) is even. Therefore, by Proposition2.2(B)(B4), we have $C'_d(\mathbb{Q}_l) \neq \emptyset$. Also for each prime l such that $l \mid D$ and $l \nmid d$, if $l \in \{D_j:\ s<j\leq n\}$, then $((\frac{d}{l})-1)((\frac{pqd}{l})-1)=0$ because $\left(\frac{d}{l}\right)\left(\frac{pqd}{l}\right)=\left(\frac{pq}{l}\right)=-1$; if $l\in\{D_i:\ 1\leq i\leq s\}$, then $\left(\frac{d}{l}\right)=(-1)^{\sharp\{\overrightarrow{lP}:\ P\in V_1\}}=1$ because (V_1,V_2) is even. So by Proposition2.2(B)(B3), we have $C'_d(\mathbb{Q}_l)\neq\emptyset$. We assert that $C'_d(\mathbb{Q}_2)\neq\emptyset$. To see this, we only need to prove the case 3 with $m=1, p\equiv 3(\mathrm{mod}4)$ and $p-D\equiv 0,6(\mathrm{mod}8)$, the other cases can be similarly done. In fact, since $2\in V_2$ and $\sharp\{\overrightarrow{2P}:\ \ P\in V_1\}$ is even, we have $d\equiv \pm 1(\mathrm{mod}8)$. So by Proposition2.2(B)(B2), $C'_d(\mathbb{Q}_2)\neq\emptyset$. This proves our assertion. So by Proposition2.2(B)(B3) and (A)(2), we obtain that $d\in S^{(\widehat{\varphi})}(E'/\mathbb{Q})$.

Conversely, suppose $d = P_1P_2\cdots P_t \in S^{(\widehat{\varphi})}(E'/\mathbb{Q})$ with distinct $P_1,\cdots,P_t \in \{-1,p,D_1,D_2,\cdots,D_n\}$. Let $V_1=\{P_1,P_2,\cdots,P_t\}$. For each prime l satisfying $l \mid \gcd(D,\ d)$, if $l\in\{D_j:\ \ s<j\leq n\}$, $\sharp\{\overrightarrow{lP}:\ P\in V_2\}$ is even because $\sharp\{\overrightarrow{lP}:\ \ P\in V_2\}=0$. If $l\in\{D_i:\ \ 1\leq i\leq s\}$, by Proposition2.2(B)(B4) and $\left(\frac{pq}{l}\right)=1$, we have $\left(\frac{-pdDl^{-2}}{l}\right)-1=0$, and so $1=\left(\frac{-pdDl^{-2}}{l}\right)=(-1)^{\sharp\{\overrightarrow{lP}:P\in V_2\}}$, which shows that $\sharp\{\overrightarrow{lP}:\ P\in V_2\}$ is even. Also, for each prime l satisfying $l\mid D$ and $l\nmid d$, if $l\in\{D_j:\ s<j\leq n\}$, then $\sharp\{\overrightarrow{lP}: P\in V_2\}$ is even because $\sharp\{\overrightarrow{lP}: P\in V_2\}=0$; if $l\in\{D_i:\ 1\leq i\leq s\}$, by Proposition2.2(B)(B3) and $\left(\frac{pq}{l}\right)=1$, we have $\left(\frac{d}{l}\right)-1=0$. So $1=\left(\frac{d}{l}\right)=(-1)^{\sharp\{\overrightarrow{lP}:\ P\in V_1\}}$, which shows that $\sharp\{\overrightarrow{lP}: P\in V_1\}$ is even. As for the vertex $l=p,-1$, by the definition of $g(+D)$, we have $\sharp\{\overrightarrow{lP}:\ \ P\in V_1\}=0$ or $\sharp\{\overrightarrow{lP}:\ P\in V_2\}=0$. Now firstly, in case 2, $-2\in V_2$. By $C'_d(\mathbb{Q}_2)\neq\emptyset$ and

the conditions for m, p, D, we have $d \equiv 1, 3(\text{mod}8)$. So $\sharp\{\overrightarrow{-2P}: P \in V_1\}$ is even. Secondly, in case 3, $2 \in V_2$. By $C'_d(\mathbb{Q}_2) \neq \emptyset$ and the conditions for m, p, D, we have $d \equiv 1, 7(\text{mod}8)$. So $\sharp\{\overrightarrow{2P}: P \in V_1\}$ is even. Lastly, in case 5, $\pm 2 \in V_2$. By $C'_d(\mathbb{Q}_2) \neq \emptyset$ and the conditions for m, p, D, we have $d \equiv 1(\text{mod}8)$. So both $\sharp\{\overrightarrow{-2P}, P \in V_1\}$ and $\sharp\{\overrightarrow{2P}: P \in V_1\}$ are even. To sum up, (V_1, V_2) is even. The Proof is completed. $\square$

Proof of Theorem 1.2. By Proposition 2.2, we have $\{1, pq, -pD, -qD\} \subset S^{(\widehat{\varphi})}(E'/\mathbb{Q})$. Then the conclusion follows easily by Lemma2.9. The proof is completed. $\square$

Definition 2.10. Let $D = D_1 D_2 \cdots D_s D_{s+1} \cdots D_n$ with $\left(\frac{pq}{D_i}\right) = 1$ $(i \leq s)$ and $\left(\frac{pq}{D_j}\right) = -1$ $(s < j \leq n)$ for some non-negative integer $s \leq n$. A directed graph $G(-D)$ is defined as follows:

Case 1. If $m = 1, D \equiv 1(\text{mod}4)$, then define the directed graph $G(-D) = G_1(-D)$ by defining the vertex $V(G(-D))$ to be $V(G_1(-D)) = \{-1, p, q, D_1, D_2, \cdots, D_n\}$ and the edges $E(G(-D))$ as $E(G_1(-D)) = \{\overrightarrow{D_i D_j}: \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s, 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_j D_i}: \left(\frac{D_i}{D_j}\right) = -1, 1 \leq i \leq s,\ s < j \leq n\} \bigcup \{\overrightarrow{l D_i}: \left(\frac{D_i}{l}\right) = -1, 1 \leq i \leq s,\ l = p, q\} \bigcup \{\overrightarrow{D_k - 1}: \left(\frac{-1}{D_k}\right) = -1, 1 \leq k \leq n\} \bigcup \{\overrightarrow{D_i p}: \left(\frac{p}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{-1 l}: \left(\frac{-1}{l}\right) = -1, l = p, q\}$.

Case 2. If m, p and D satisfy one of the following conditions:

(1) $m = 1, D \equiv 3(\text{mod}4)$. (2) $m = 2, D \equiv 3(\text{mod}4)$ and $(p+2)D \not\equiv 3(\text{mod}8)$, then define the directed graph $G(-D) = G_2(-D)$ by defining the vertex $V(G(-D))$ to be $V(G_2(-D)) = \{-1, p, q, D_1, D_2, \cdots, D_n\}$ and the edges $E(G(-D))$ as

$E(G_2(-D)) = \{\overrightarrow{D_i D_j}: \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s,\ 1 \leq j \leq n\} \bigcup \{\overrightarrow{D_j D_i}: \left(\frac{D_i}{D_j}\right) =$

$-1, 1 \le i \le s, s < j \le n\} \bigcup \{\overrightarrow{lD_i} : \left(\frac{D_i}{l}\right) = -1, 1 \le i \le s,\ l = p, q\} \bigcup \{\overrightarrow{-1D_k} : \left(\frac{-1}{D_k}\right) = -1, 1 \le k \le n\} \bigcup \{\overrightarrow{D_i p} : \left(\frac{p}{D_i}\right) = -1, 1 \le i \le s\} \bigcup \{\overrightarrow{l-1} : \left(\frac{-1}{l}\right) = -1,\ l = p, q\}$.

Case 3. If m, p and D satisfy one of the following conditions:

(1) $m = 2, (p+2)D \equiv 3(\mathrm{mod} 8)$; (2) $m \ge 3, pD \equiv 1(\mathrm{mod} 4)$,

then define the directed graph $G(-D) = G_3(-D)$ by defining the vertex $V(G(-D))$ to be $V(G_3(-D)) = \{-1, p, q, D_1, D_2, \cdots, D_n\}$ and the edges $E(G(-D))$ as

$E(G_3(-D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \le i \le s, 1 \le j \le n\} \bigcup \{\overrightarrow{D_jD_i} : \left(\frac{D_i}{D_j}\right) = -1, 1 \le i \le s,\ s < j \le n\} \bigcup \{\overrightarrow{lD_i} : \left(\frac{D_i}{l}\right) = -1, 1 \le i \le s, l = p, q\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \le i \le s\} \bigcup \{\overrightarrow{D_k - 1} : \left(\frac{-1}{D_k}\right) = -1, 1 \le k \le n\} \bigcup \{\overrightarrow{l-1} : \left(\frac{-1}{l}\right) = -1, l = p, q\}$.

Case 4. If $m = 2, (p+2)D \not\equiv 3(\mathrm{mod} 8)$ and $D \equiv 1(\mathrm{mod} 4)$, define the directed graph $G(-D) = G_4(-D)$ by defining the vertex $V(G(-D))$ to be $V(G_4(-D)) = \{-1, p, q, D_1, D_2, \cdots, D_n\}$ and the edges $E(G(-D))$ as

$E(G_4(-D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \le i \le s, 1 \le j \le n\} \bigcup \{\overrightarrow{D_jD_i} : \left(\frac{D_i}{D_j}\right) = -1, 1 \le i \le s,\ s < j \le n\} \bigcup \{\overrightarrow{lD_i} : \left(\frac{D_i}{l}\right) = -1, 1 \le i \le s,\ l = p, q\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \le i \le s\} \bigcup \{\overrightarrow{D_k - 1} : \left(\frac{-1}{D_k}\right) = -1, 1 \le k \le n\} \bigcup \{\overrightarrow{l-1} : \left(\frac{-1}{l}\right) = -1, l = p, q\} \bigcup \{\overrightarrow{-1p}\}$.

Case 5. If $m \ge 3, pD \equiv 3(\mathrm{mod} 4)$, define the directed graph $G(-D) = G_5(-D)$ by defining the vertex $V(G(-D))$ to be $V(G_5(-D)) = \{-1, p, q, D_1, D_2, \cdots, D_n\}$ and the edges $E(G(-D))$ as

$E(G_5(-D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \le i \le s, 1 \le j \le n\} \bigcup \{\overrightarrow{D_jD_i} : \left(\frac{D_i}{D_j}\right) = -1, 1 \le i \le s,\ s < j \le n\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \le i \le s\} \bigcup \{\overrightarrow{lD_i} : \left(\frac{D_i}{l}\right) =$

$-1, 1 \leq i \leq s, l = p, q\} \bigcup \{\overline{D_k - 1} : \left(\frac{-1}{D_k}\right) = -1, 1 \leq k \leq n\} \bigcup \{\overrightarrow{l - 1} : \left(\frac{-1}{l}\right) = -1, l = p, q\} \bigcup \{\overrightarrow{-1p} : \left(\frac{-1}{p}\right) = -1\}$.

Here we define $\left(\frac{2}{-1}\right) = 1$, if m, p and D satisfy one of the following conditions:

(1) $m = 1,\ pD \equiv 7(\mathrm{mod} 8)$ and $D \equiv 1(\mathrm{mod} 4)$;

(2) $m = 1,\ pD \equiv 1(\mathrm{mod} 8)$ and $D \equiv 3(\mathrm{mod} 4)$; (3) $m = 3, pD \equiv 1(\mathrm{mod} 8)$;

(4) $m \geq 4,\ pD \equiv 7(\mathrm{mod} 8)$; (5) $m \geq 5, pD \equiv 1(\mathrm{mod} 8)$.

And we define $\left(\frac{2}{-1}\right) = -1$, if m, p and D satisfy one of the following conditions:

(1) $m = 1,\ pD \equiv 1(\mathrm{mod} 8)$ and $D \equiv 1(\mathrm{mod} 4)$;

(2) $m = 1,\ pD \equiv 3(\mathrm{mod} 8)$ and $D \equiv 3(\mathrm{mod} 4)$; (3) $m \geq 4, pD \equiv 3(\mathrm{mod} 8)$.

Lemma 2.11. For every even partition (V_1, V_2) of $G(-D)$ such that V_1 contains no p, q or D_k $(s < k \leq n)$, we have $d \in S^{(\varphi)}(E/\mathbb{Q})$, where $d = \prod_{P_0 \in V_1} P_0$. Conversely, if d is odd and $d \in S^{(\varphi)}(E/\mathbb{Q})$, we may write $d = \delta P_1 P_2 \cdots P_t$ for $\delta = \pm 1$ and distinct $P_j \in V(G(-D))$ $(1 \leq j \leq t)$, then (V_1, V_2) is even. Here

$$V_1 = \begin{cases} \{P_1, P_2, \cdots, P_t\} & \text{if } \delta = 1, \\ \{-1, P_1, P_2, \cdots, P_t\} & \text{if } \delta = -1. \end{cases}$$

Proof. Similar to the proof of Lemma 2.6.

Lemma 2.12. For every quasi-even partition (V_1, V_2) of $G(-D)$ such that V_1 contains no p, q or D_k $(s < k \leq n)$, we have $2d \in S^{(\varphi)}(E/\mathbb{Q})$, where $d = \prod_{P_0 \in V_1} P_0$. Conversely, if d is even and $d \in S^{(\varphi)}(E/\mathbb{Q})$, we may write $d = 2\delta P_1 P_2 \cdots P_t$ for $\delta = \pm 1$ and distinct $P_j \in V(G(-D))$ $(1 \leq j \leq t)$, then (V_1, V_2) is quasi-even. Here

$$V_1 = \begin{cases} \{P_1, P_2, \cdots, P_t\} & \text{if } \delta = 1, \\ \{-1, P_1, P_2, \cdots, P_t\} & \text{if } \delta = -1. \end{cases}$$

Proof. Similar to the proof of Lemma 2.7.

Definition 2.13. Let $D = D_1 D_2 \cdots D_s D_{s+1} \cdots D_n$ with $\left(\frac{pq}{D_i}\right) = 1$ $(i \leq s)$

and $\left(\frac{pq}{D_j}\right)=-1$ $(s<j\leq n)$ for some non-negative integer $s\leq n$. A graph directed $g(-D)$ is defined as follows:

Case 1. If m,p and D satisfy one of the following conditions:

(1) $m=1, p-D\equiv 2,4(\bmod 8)$;

(2) $m=2, pD\equiv 3(\bmod 4)$; (3) $m=2, D\equiv 1(\bmod 4)$; and $pD\equiv 5(\bmod 8)$;

(4) $m=2, D\equiv 3(\bmod 4)$ and $pD\equiv 1(\bmod 8)$; (5) $m=3, pD\equiv 3(\bmod 4)$,

then define the directed graph $g(-D)=g_1(-D)$ by defining the vertex $V(g(-D))$ to be $V(g_1(-D))=\{p, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(-D))$ as $E(g_1(-D))$ $=\{\overrightarrow{D_iD_j}:\ \left(\frac{D_j}{D_i}\right)=-1, 1\leq i\leq s, 1\leq j\leq n\}\bigcup\{\overrightarrow{D_ip}:\ \left(\frac{p}{D_i}\right)=-1, 1\leq i\leq s\}$.

Case 2. If m,p and D satisfy one of the following conditions:

(1) $m=1, p\equiv 1(\bmod 4)$ and $p-D\equiv 0,6(\bmod 8)$; (2) $m\geq 4, pD\equiv 3(\bmod 8)$, then define the directed graph $g(-D)=g_2(-D)$ by defining the vertex $V(g(-D))$ to be $V(g_2(-D))=\{p,-2, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(-D))$ as $E(g_2(-D))$ $=\{\overrightarrow{D_iD_j}:\ \left(\frac{D_j}{D_i}\right)=-1, 1\leq i\leq s, 1\leq j\leq n\}\bigcup\{\overrightarrow{-2p}:\ \left(\frac{-2}{p}\right)=-1\}\bigcup\{\overrightarrow{D_ip}:$ $\left(\frac{p}{D_i}\right)=-1, 1\leq i\leq s\}\bigcup\{\overrightarrow{-2D_k}:\ \left(\frac{-2}{D_k}\right)=-1, 1\leq k\leq n\}$

Case 3. If m,p and D satisfy one of the following conditions:

(1) $m=1, p\equiv 3(\bmod 4)$ and $p-D\equiv 0,6(\bmod 8)$; (2) $m\geq 5, pD\equiv 7(\bmod 8)$, then define the directed graph $g(-D)=g_3(-D)$ by defining the vertex $V(g(-D))$ to be $V(g_3(-D))=\{p,2, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(-D))$ as $E(g_3(-D))$ $=\{\overrightarrow{D_iD_j}:\ \left(\frac{D_j}{D_i}\right)=-1, 1\leq i\leq s, 1\leq j\leq n\}\bigcup\{\overrightarrow{2p}:\ \left(\frac{2}{p}\right)=-1\}\bigcup\{\overrightarrow{D_ip}:$ $\left(\frac{p}{D_i}\right)=-1, 1\leq i\leq s\}\bigcup\{\overrightarrow{2D_k}:\ \left(\frac{2}{D_k}\right)=-1, 1\leq k\leq n\}$.

Case 4. If m,p and D satisfy one of the following conditions:

(1) $m=2, D\equiv 1(\bmod 4)$ and $pD\equiv 1(\bmod 8)$; (2) $m=2, D\equiv 3(\bmod 4)$ and

$pD \equiv 5(\mathrm{mod}8)$; (3) $m \geq 3, pD \equiv 5(\mathrm{mod}8)$; (4) $m = 4, pD \equiv 1(\mathrm{mod}8)$, then define the directed graph $g(-D) = g_4(-D)$ by defining the vertex $V(g(-D))$ to be $V(g_4(-D)) = \{p, -1, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(-D))$ as

$E(g_4(-D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, 1 \leq i \leq s,\ 1 \leq j \leq n\} \bigcup \{\overrightarrow{-1p} : \left(\frac{-1}{p}\right) = -1\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{-1D_k} : \left(\frac{-1}{D_k}\right) = -1, 1 \leq k \leq n\}$.

Case 5. If m, p and D satisfy one of the following conditions:

(1) $m = 3, pD \equiv 1(\mathrm{mod}8)$; (2) $m \geq 5, pD \equiv 1(\mathrm{mod}8)$, then define the directed graph $g(-D) = g_5(-D)$ by defining the vertex $V(g(-D))$ to be $V(g_5(-D)) = \{p, -1, 2, D_1, D_2, \cdots, D_n\}$ and the edges $E(g(-D))$ as

$E(g_5(-D)) = \{\overrightarrow{D_iD_j} : \left(\frac{D_j}{D_i}\right) = -1, l \leq i \leq s,\ 1 \leq j \leq n\} \bigcup \{\overrightarrow{-1p} : \left(\frac{-1}{p}\right) = -1\} \bigcup \{\overrightarrow{D_ip} : \left(\frac{p}{D_i}\right) = -1, 1 \leq i \leq s\} \bigcup \{\overrightarrow{-1D_k} : \left(\frac{-1}{D_k}\right) = -1,\ 1 \leq k \leq n\} \bigcup \{\overrightarrow{2D_k} : \left(\frac{2}{D_k}\right) = -1, 1 \leq k \leq n\} \bigcup \{\overrightarrow{2p} : \left(\frac{2}{p}\right) = -1\}$.

Lemma 2.14. For every even partition (V_1, V_2) of $g(-D)$ such that V_1 contains no $-1, \pm 2$, we have $d \in S^{(\widehat{\varphi})}(E'/\mathbb{Q})$, where $d = \prod_{P_0 \in V_1} P_0$. Conversely, if d is odd and $d \in S^{(\widehat{\varphi})}(E'/\mathbb{Q})$, we may write $d = P_1P_2\cdots P_t$ for distinct $P_j \in V(g(-D))$ $(1 \leq j \leq t)$, then (V_1, V_2) is even, where $V_1 = \{P_1, P_2, \cdots, P_t\}$.

Proof. Similar to the proof of Lemma 2.9.

Proofs of Theorem 1.3 and 1.4. By using Proposition 2.3, 2.4 and Lemma 2.11, 2.12, 2.14, the proofs are similar to that of Theorem 1.1 and 1.2. $\square$

Appendix

In this appendix, by descent method, we obtain the following results about Selmer group of the elliptic curve (1.1) for all integers $m \geq 2$, which generalize the

ones in [LQ] for the case $m=1$. The method is the same as in [LQ] (see also [QZ] and [DW]), so we omit the details.

Theorem A.1. Let $E=E_+$ be the elliptic curve in (1.1) with $\varepsilon=+1$ and l be an odd prime number. For each $i\in\{1,\cdots,n\}$, denote

$\Pi_i^+(D)=\delta_i+\left(1-\left(\frac{q\widehat{D}_i}{D_i}\right)\right)\left(1-\left(\frac{p\widehat{D}_i}{D_i}\right)\right)+\sum_{l|pq\widehat{D}_i}\left(1-\left(\frac{D_i}{l}\right)\right),$

where $\delta_i=0$ if D_i,m,p and D satisfy one of the following conditions:

(1) $D_i\equiv 1(\text{mod }4)$, (2) $m=2, p-D\equiv 2(\text{mod }8)$, (3) $m\geq 3, p+D\equiv 0(\text{mod }4)$; otherwise, $\delta_i=1$. And denote

$$\Pi_{n+1}^+(D)=\delta_{n+1}+\sum_{l|pqD}\left(1-\left(\frac{2}{l}\right)\right),$$

where $\delta_{n+1}=0$, if m,p and D satisfy one of the following conditions:

(1) $m=3, pD\equiv -1(\text{mod }8)$, (2) $m=4, pD\equiv 1(\text{mod }8)$, (3) $m\geq 5$; otherwise, $\delta_{n+1}=1$. Here $(-)$ is the (Legendre) quadratic residue symbol. And define a function $\rho^+(D)$ by

$$\rho^+(D)=\sum_{i=1}^{n+1}\left[\frac{1}{1+\Pi_i^+(D)}\right],$$

where [x] is the greatest integer $\leq x$. Then there exists a subset $T\subset\{2,D_1,\cdots,D_n\}$ with cardinal $\sharp T=\rho^+(D)$ such that $S^{(\varphi)}(E/\mathbb{Q})\supset<T\text{mod}(\mathbb{Q}^{\star^2})>\cong(\mathbb{Z}/2\mathbb{Z})^{\rho^+(D)}$. In particular, $\dim_2 S^{(\varphi)}(E/\mathbb{Q})\geq\rho^+(D)$.

Theorem A.2. Let $E'=E'_+$ be the elliptic curve in (1.2) with $\varepsilon=+1$. For each $i\in Z(n)=\{1,\cdots,n\}$, denote

$\Pi_i^+(D')=\left(1-\left(\frac{-q\widehat{D}_i}{D_i}\right)\right)\left(1-\left(\frac{-p\widehat{D}_i}{D_i}\right)\right)+\sum_{j=1,\ j\neq i}^{n}\left(1-\left(\frac{D_i}{D_j}\right)\right)\left(1-\left(\frac{pqD_i}{D_j}\right)\right)$ and $\Pi_{n+1}^+(D')=\delta'_{n+1}+\sum_{i=1}^{n}\left(1-\left(\frac{-1}{D_i}\right)\right)\left(1-\left(\frac{-pq}{D_i}\right)\right)$, where $\delta'_{n+1}=0$, if m,p and D satisfy one of the following conditions: (1) $m=2, p-D\not\equiv 2(\text{mod }8)$,

(2) $m=3, p-D\equiv 0(\bmod\ 4)$, (3) $m\geq 4, p-D\equiv 0(\bmod\ 8)$;

otherwise, $\delta'_{n+1}=1$. Here $(-)$ is the (Legendre) quadratic residue symbol.

Take a subset I of $Z(n)$ as follows:

if $m=2$, set $I=\{i\in Z(n):\ D_i\equiv 1(\mathrm{mod}4)\}\bigcup\{i\in Z(n):\ D_i+pD\equiv 0(\mathrm{mod}4)\}\bigcup\{i\in Z(n): D_i\equiv 3(\mathrm{mod}4)$ and $p-D\equiv 6(\mathrm{mod}8)\}$;

if $m=3$, set $I=\{i\in Z(n):\ D_i\equiv 1(\mathrm{mod}8)\}\bigcup\{i\in Z(n):\ D_i+pD\equiv 0(\mathrm{mod}8)\}\bigcup\{i\in Z(n):\ D_i\equiv 3(\mathrm{mod}4)$ and $pD+D_i\equiv 4(\mathrm{mod}8)\}\bigcup\{i\in Z(n):\ D_i\equiv 5(\mathrm{mod}8)$ and $pD-D_i\equiv 0(\mathrm{mod}4)\}$;

if $m=4$, set $I=\{i\in Z(n):\ D_i\equiv 1(\mathrm{mod}8)\}\bigcup\{i\in Z(n):\ D_i+pD\equiv 0(\mathrm{mod}8)\}\bigcup\{i\in Z(n):\ D_i\equiv 5(\mathrm{mod}8)$ and $pD+D_i\equiv 4(\mathrm{mod}8)\}$;

if $m\geq 5$, set $I=\{i\in Z(n):\ D_i\equiv 1(\mathrm{mod}8)\}\bigcup\{i\in Z(n):\ D_i+pD\equiv 0(\mathrm{mod}8)\}$.

Define a function $\rho^+(D')$ by

$$\rho^+(D')=\sum_{i\in I\bigcup\{n+1\}}\left[\frac{1}{1+\Pi_i^+(D')}\right],$$

where [x] is the greatest integer $\leq x$. Then there exists a subset $T\subset\{-1,D_1,\cdots,D_n\}$ with cardinal $\sharp T=\rho^+(D')$ such that $S^{(\varphi)}(E/\mathbb{Q})\supset <T\mathrm{mod}(\mathbb{Q}^{\star^2})>\cong(\mathbb{Z}/2\mathbb{Z})^{\rho^+(D')}$. In particular, $\dim_2 S^{(\varphi)}(E/\mathbb{Q})\geq\rho^+(D')$.

Theorem A.3. Let $E=E_-$ be the elliptic curve in (1.1) with $\varepsilon=-1$ and l be an odd prime number. For each $i\in\{1,\cdots,n\}$, denote

$\Pi_i^-(D)=\delta_i+\left(1-\left(\frac{-q\widehat{D_i}}{D_i}\right)\right)\left(1-\left(\frac{-p\widehat{D_i}}{D_i}\right)\right)+\sum_{l|pq\widehat{D_i}}\left(1-\left(\frac{D_i}{l}\right)\right)$, where $\delta_i=0$, if D_i, m, p and D satisfy one of the following conditions:

(1) $D_i\equiv 1(\mathrm{mod}4)$, (2) $m=2, p+D\equiv 2(\mathrm{mod}8)$, (3) $m\geq 3, p-D\equiv 0(\mathrm{mod}4)$;

otherwise, $\delta_i = 1$. And denote

$$\Pi_{n+1}^{-}(D) = \delta_{n+1} + \sum_{l|pqD} \left(1 - \left(\frac{2}{l}\right)\right),$$

where $\delta_{n+1} = 0$, if m, p and D satisfy one of the following conditions:

(1) $m = 3, pD \equiv 1(\text{mod}8)$, (2) $m = 4, pD \equiv -1(\text{mod}8)$, (3) $m \geq 5$; otherwise, $\delta_{n+1} = 1$; and denote

$$\Pi_{n+2}^{-}(D) = \delta_{n+2} + \sum_{l|pqD} \left(1 - \left(\frac{-1}{l}\right)\right),$$

where $\delta_{n+2} = 0$, if m, p and D satisfy one of the following conditions:

(1) $pD \equiv 1(\text{mod}8)$, (2) $m \geq 3, pD \equiv 5(\text{mod}8)$; otherwise, $\delta_{n+2} = 1$.

And define a function $\rho^{-}(D)$ by

$$\rho^{-}(D) = \sum_{i=1}^{n+2} \left[\frac{1}{1 + \Pi_i^{-}(D)}\right],$$

where [x] is the greatest integer $\leq x$. Then there exists a subset $T \subset \{-1, 2, D_1, \cdots, D_n\}$ with cardinal $\sharp T = \rho^{-}(D)$ such that $S^{(\varphi)}(E/\mathbb{Q}) \supset < \{D_i : \ D_i \in T\} \text{ mod } (\mathbb{Q}^{\star^2}) > \cong (\mathbb{Z}/2\mathbb{Z})^{\rho^{-}(D)}$. In particular, $\dim_2 S^{(\varphi)}(E/\mathbb{Q}) \geq \rho^{-}(D)$.

Theorem A.4. Let $E' = E'_{-}$ be the elliptic curve in (1.2) with $\varepsilon = -1$. For each $i \in Z(n) = \{1, \cdots, n\}$, denote $\Pi_i^{-}(D') = \left(1 - \left(\frac{q\widehat{D_i}}{D_i}\right)\right)\left(1 - \left(\frac{p\widehat{D_i}}{D_i}\right)\right) + \sum_{j=1,\ j\neq i}^{n} \left(1 - \left(\frac{D_i}{D_j}\right)\right)\left(1 - \left(\frac{pqD_i}{D_j}\right)\right)$. Here $(-)$ is the (Legendre) quadratic residue symbol. Take a subset I of $Z(n)$ as follows:

if $m = 2$, set $I = \{i \in Z(n) : \ D_i \equiv 1(\text{mod}4)\} \bigcup \{i \in Z(n) : \ D_i - pD \equiv 0(\text{mod}4)\} \bigcup \{i \in Z(n) : \ D_i \equiv 3(\text{mod}4) \text{ and } p + D \equiv 6(\text{mod}8)\}$;

if $m = 3$, set $I = \{i \in Z(n) : \ D_i \equiv 1(\text{mod}8)\} \bigcup \{i \in Z(n) : \ D_i - pD \equiv 0(\text{mod}8)\} \bigcup \{i \in Z(n) : \ D_i \equiv 3(\text{mod}4) \text{ and } pD - D_i \equiv 4(\text{mod}8)\}$

$\bigcup\{i \in Z(n) : D_i \equiv 5(\mathrm{mod}8)$ and $pD + D_i \equiv 0(\mathrm{mod}4)\}$;

if $m = 4$, set $I = \{i \in Z(n) : \ D_i \equiv 1(\mathrm{mod}8)\} \bigcup \{i \in Z(n) : \ D_i - pD \equiv 0(\mathrm{mod}8) \bigcup \{i \in Z(n) : \ D_i \equiv 5(\mathrm{mod}8)$ and $pD - D_i \equiv 4(\mathrm{mod}8)\}$;

if $m \geq 5$, set $I = \{i \in Z(n) : \ D_i \equiv 1(\mathrm{mod}8)\} \bigcup \{i \in Z(n) : \ D_i - pD \equiv 0(\mathrm{mod}8)\}$.

Define a function $\rho^-(D')$ by

$$\rho^-(D') = \sum_{i \in I} \left[\frac{1}{1 + \Pi_i^-(D')}\right],$$

where [x] is the greatest integer $\leq x$. Then there exists a subset $T \subset \{D_1, \cdots, D_n\}$ with cardinal $\sharp T = \rho^-(D')$ such that $S^{(\varphi)}(E/\mathbb{Q}) \supset < T \bmod (\mathbb{Q}^{\star^2}) > \cong (\mathbb{Z}/2\mathbb{Z})^{\rho^-(D')}$. In particular, $\dim_2 S^{(\varphi)}(E/\mathbb{Q}) \geq \rho^-(D')$.

Acknowledgement We are grateful to Prof. Keqin Feng for sending us his papers [F1], [F2], [FX] and other materials which are helpful for this work.

References

[**DW**] A. Dabrowski, M. Wieczorek, On the equation $y^2 = x(x - 2^m)(x + q - 2^m)$, J. Number Theory, 2007, 124: 364-379.

[**F1**] K. Feng, Non-congruent number, odd graphs and the BSD conjecture, Acta Arith., 1996, 80: 71-83.

[**F2**] K. Feng, Non-Congruent Numbers and Elliptic Curves with Rank Zero (in Chinese), University of Science and Technology of China Press, 2008.

[**FJ**] B. Faulkner, K. James, A graphical approach to computing Selmer groups of congruent number curves, Ramanujan J., 2007, 14: 107-129.

[**FX**] K. Feng, M. Xiong, On elliptic curves $y^2 = x^3 - n^2x$ with rank zero, J. Number Theory, 2004, 109: 1-24.

[**LQ**] F. Li, D. Qiu, On Several Families of Elliptic Curves with Arbitrary Large Selmer Groups, arXiv.org: 0911.0236v1 [math.AG] 2 Nov 2009.

[**QZ**] D. Qiu, X. Zhang, Mordell-weil groups and selmer groups of two types of elliptic curves, Science in China (series A), 2002, Vol.45, No.11, 1372-1380.

[**S**] J. Silverman, The Arithmetic of Elliptic Curves, New York: Springer-Verlag, 1986.